Carnegie Mellon University
Software Engineering Institute

Security for a Public Web Site

Robert Firth
Gary Ford
Barbara Fraser
John Kochmar
Suresh Konda
John Richael
Derek Simmel
Networked Systems Survivability Program

Lisa Cunningham
Computer Sciences Corporation

August 1997

Security Improvement Module
CMU/SEI-SIM-002

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of, "Don't ask, don't tell, don't pursue," excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Security Improvement Module
CMU/SEI-SIM-002
August 1997

Security for a Public Web Site

Robert Firth
Gary Ford
Barbara Fraser
John Kochmar
Suresh Konda
John Richael
Derek Simmel
Networked Systems Survivability Program

Lisa Cunningham
Computer Sciences Corporation

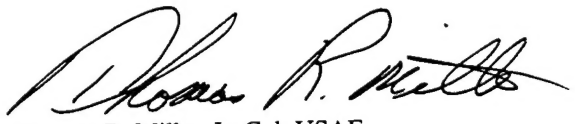
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

This report was prepared for the

SEI Joint Program Office
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Thomas R. Miller, Lt Col, USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

This document is available through SAIC/ASSET: 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone: (304) 284-9000 / FAX: (304) 284-9001 / World Wide Web: http://www.saic.com/-contact.html / e-mail: webmaster@cpqm.saic.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218. Phone: (703) 767-8274 or toll-free in the U.S. — 1-800 225-3842).

Table of Contents

Preface

This document is one of a new series of publications of the Software Engineering Institute at Carnegie Mellon University—*security improvement modules*. They are intended to provide concrete, practical guidance that will help organizations improve the security of their networked computer systems.

Module structure

Each module addresses an important but relatively narrowly defined problem in network security. The first section of the module describes the problem and outlines a set of *security improvement practices* to help solve it. Each practice is a recommended way of performing common tasks related to the secure operation of networked computer systems.

The remaining sections of the module are detailed descriptions of the practices. Each includes a rationale for the recommended actions and a step-by-step description of how to perform them.

Intended audience

The practices are written for system and network administrators within an organization. These are the people whose day to day activities include installation, configuration, and maintenance of the computers and networks.

Revised versions

Network technologies continue to evolve rapidly, leading to both new solutions and new problems in security. We expect that modules and practices will need to be revised from time to time. To permit more timely publication of the most up-to-date versions, the modules and practices are also being published on the World Wide Web. At the end of each section of this document is the URL of its Web version.

Implementation details

How an organization adopts and implements the practices often depends on the specific networking and computing technologies it uses. For some practices, technology-specific implementation details have been written and are being published on the World Wide Web. The Web version of each practice contains links to the implementation details.

Security for a Public Web Site

The World Wide Web is one of the most important ways for organizations to publish information. Unfortunately, if you are not careful in setting up and operating a public Web site, you leave yourself and your organization vulnerable to a variety of security problems. You could find yourself in an embarrassing situation because malicious intruders have changed the content of your Web pages. Public Web sites have also been the entry point for intrusions into organization's internal networks for the purpose of accessing confidential information. The practices recommended below are designed to help you prevent these and several other known security problems.

Who should read these practices

These practices are applicable to your organization if you intend to operate your own Web site to make information public to the entire Internet community.

We assume that you have these security requirements for your Web site:

- You want to maintain the integrity of the information intended to be published.
- You want to prevent the use of the Web host[1] as a staging area for intrusions into your organization's network that could result in breaches of confidentiality, integrity, or availability of information resources.
- You want to prevent the use of the Web host as a staging area for intrusions into external sites, which could result in your organization being held liable for damages.

What these practices do not cover

These practices do not cover all aspects of using the Web in your organization. In particular, they do not address

1. Throughout these practices, we use terms such as *host* and *host machine* to refer to the hardware and operating system that will support a Web site. The term *server software* refers to the application software that implements the http protocol, and the term *server* generally means the combined hardware, operating system, and server software.

- security considerations related to Web client (browser) software
- commercial transactions via the Web
- special considerations for very large Web sites with multiple hosts
- contracting for or offering Web-hosting services (such as that offered by a commercial Internet service provider)
- other public information services, such as those based on the file transfer protocol (ftp)

Security issues

There are two main security issues related to the operation of a public Web site:

1. Improper configuration or operation of the Web server can result in the inadvertent disclosure of confidential information. This can include
   - information assets of your organization
   - information about the configuration of the server or network that could be exploited for subsequent attacks
   - information about who requested which documents from the server
2. The host used for your Web server might be compromised. That could allow intruders to
   - change the information stored on the Web server host machine, particularly the information you intend to publish
   - gain unauthorized access to resources elsewhere in your organization's computer network
   - launch attacks on external sites from your server host machine, thus concealing the intruders' identities, and perhaps making your organization liable for damages

Security improvement approach

To improve the security of your public Web site, we recommend a three-step approach. It requires implementing security practices in these areas:

1. *selecting* server and host technology
2. *configuring* server software and the underlying host technology
3. *operating* the server

In addition, we recommend that you establish security policies that mandate appropriate practices for network administrators and users. For example, you may want to establish a policy that requires system and network administrators to adopt and implement several of the practices described in this recommendation.

Summary of recommended practices

Area	Recommended Practice
Selecting server technology	1. Include explicit security requirements when selecting server and host technologies.
Configuring server technology	2. Isolate the Web server from your organization's internal network. 3. Maintain the authoritative copy of your Web site content on a more secure host. 4. Offer only essential network services and operating system services on the server host machine. 5. Configure the Web server to enhance security. 6. Consider the security implications when choosing external programs that the server can execute.
Operating the server	7. Administer the Web server in a secure manner. 8. Look for unexpected changes to directories and files. 9. Inspect your system and network logs.

Abbreviations used in these practices

DNS	domain name service
cgi, CGI	common gateway interface
ftp	file transfer protocol
http	hypertext transfer protocol
IP	Internet protocol
NIS	Network Information System
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	uniform resource locator

Where to find updates

The latest version of this module is available on the Web at URL

`http://www.cert.org/security-improvement/modules/m02.html`

1 *Include explicit security requirements when selecting server and host technologies.*

It is common to consider factors such as functionality, price, performance, and capacity when selecting computing technology. When you specify the requirements for selecting server technologies for your organization (including the host machine hardware, operating system, and server software), you should also include security requirements.

Why this is important

There are many vendors of server technologies, whose products vary with respect to security capabilities. Many known and frequently exploited vulnerabilities of network servers apply only to certain technologies. If you consider security requirements when selecting server technologies, you may be able to choose technologies with fewer vulnerabilities or better security-related features, which would permit you to have a substantially more secure site. This makes the long-term operation of your site more economical, because you can reduce the costs associated with intrusions and recovery.

Background information

The selection of Web server technology requires you to make tradeoffs among the competing requirements. To do this, you must first understand your organization's requirements.

For a Web server, the significant performance requirements are the response time (typically measured in terms of the number of connections per second that the server will allow) and throughput (typically measured in terms of the number of bytes per second of data that can be delivered to the network).

Typical functionality requirements include the ability to serve static Web pages and various forms of dynamic pages, the ability to receive and process user information (such as that supplied through forms), and the ability to provide a site search service. In addition, you may want the ability to administer the server software and the host system from another host on your network.

Security requirements typically include the following:

- the lack of vulnerability to known forms of attack against Web server hosts
- the ability to restrict administrative activities to authorized users only
- the ability to deny access to information on the server other than that intended to be published
- the ability to disable unnecessary network services that may be built into the operating system or server software

- the ability to control access to various forms of external executable programs (such as cgi scripts and server plug-ins)
- the ability to log appropriate Web server activities for purposes of detecting intrusions and attempted intrusions

How to do it

➤ *Identify your functionality and performance requirements.*

➤ *Review the recommended practices that address the configuration and operation of the server technology. Note the kinds of security problems that those practices are intended to help you avoid.*

➤ *Where available, look at the sample implementations of those practices. Note whether the implementations for a particular technology are simple or complex, inexpensive or costly.*

➤ *Based on your organization's security needs, identify specific security-related features that you want in the server technology you will be selecting.*

➤ *Check with available sources of incident data to help determine the likelihood of particular kinds of incidents and the vulnerabilities of specific servers.*

➤ *Identify candidate technologies that meet your functionality, performance, and security requirements.*

➤ *Estimate the differences in operating costs of competing technologies, including the business costs of potential security incidents.*

➤ *Select the technology that you believe offers the best balance of functionality, performance, security, and overall cost.*

Policy considerations

Your organization's networked systems security policy should:

- Require a security evaluation as part of your computing and network technology selection procedures.

In addition, we recommend that your organization's purchasing guidelines mandate the specification of security requirements for all computing and network technologies.

Other information

CERT®[1] advisories and summaries[2] from time to time include information on new vulnerabilities in Web server software and the operating systems under which they operate.

1. Registered in the U.S. Patent and Trademark Office.
2. See http://www.cert.org and ftp://info.cert.org/pub/cert_advisories/ .

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p009.html`

2 *Isolate the Web server from your organization's internal network.*

You usually have several choices of where to place a public Web server on your organization's network. We recommend that it be placed on a separate subnetwork, so that traffic between the Internet and the server does not traverse any part of your private internal network and no internal network traffic is visible to the server.

Why this is important

A public Web server host is a computer that is meant for public access. This means that there will be many people who will access the host (and its stored information) from locations all over the world. Regardless of how well the host computer and its application software are configured, there is always the chance that someone will discover a new vulnerability, exploit it, and gain unintended access to the Web server host (e.g., user account or privileged account on a host with a multiuser operating system). If that happens, you need to prevent these events:

- The intruder is able to observe or capture network traffic that is flowing between internal hosts. Such traffic might include authentication information, proprietary business information, personnel data, and many other kinds of sensitive data.
- The intruder is able to get to internal hosts, or to obtain detailed information about them.

To guard against these two threats, the server host must be isolated from the internal network and its traffic.

How to do it

➤ *Place the host on a subnet isolated from the main internal network.*

The recommended configuration is shown in the Figure 1.

➤ *Use filters or a firewall to restrict traffic from the Web server host to the internal network.*

➤ *Turn off source routing at the router so that the Web server host cannot be used to forward packets to hosts in the internal network.*

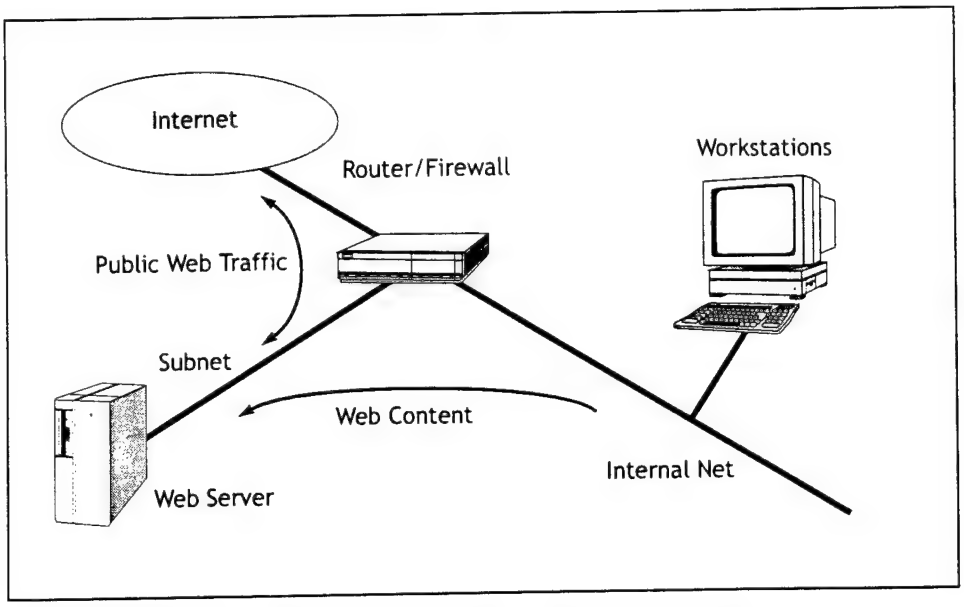


Figure 1: Network structure for the Web server

Policy considerations

Your organization's networked systems security policy should

- Require the placement of public servers on subnets separate from internal networks.
- Require that routers be configured to restrict traffic from public servers to internal networks.

Other information

There are other approaches that will address the threats mentioned above, but they are not recommended.

For example, we might place the Web server on the internal network and then use smart hubs to separate it from internal network traffic. We might also choose to encrypt all internal traffic, so that even if the server is compromised, any traffic it sees will not be readable. But neither of these methods prevents traffic from the Web server host to other hosts on the internal network.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p010.html`

3 *Maintain the authoritative copy of your Web site content on a more secure host.*

If the integrity of the public information on your server is ever compromised, you need an authoritative copy from which to restore it. We recommend that the authoritative (genuine and correct) copy of that information be kept on a host separate from and more secure than the Web server host (e.g., one that is located on an internal subnet inside your network firewall).

Why this is important

The authoritative copy of public information stored on a more secure host is less likely to be compromised by a malicious intruder, and it is therefore more likely to be available whenever needed to restore the public copy.

This approach can also simplify some administrative tasks. For example, it makes it unnecessary to perform file backups on the public server (for security reasons, the backup files would need to be kept on a separate host anyway). It also enables maintenance and creation of Web site content to be contained on the internal subnet.

How to do it

➤ *The goal is that the authoritative copy be inaccessible to all unauthorized users (internal or external). You can choose any implementation of this practice that achieves that goal.*

Typically, the authoritative copy is kept on a host accessible to the Web site administrator, and perhaps also to the people in your organization who are responsible for the creation and maintenance of Web content. This is likely to be on your organization's internal network.

Policy considerations

Your organization's networked systems security policy should

- Require that information on public servers has authoritative copies stored on more secure hosts.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p011.html`

4 *Offer only essential network services and operating system services on the server host machine.*

Ideally, the Web server should be on a dedicated, single-purpose host. Many modern computers are configured "out of the box" to provide a wider set of services and applications than strictly required to provide Web services. Hence, explicit configuration may be required to eliminate or disable unnecessary services and applications.

Why this is important

Offering only the essential network services on a particular host can enhance your network security in several ways:

- Other services cannot be used to attack the host and impair or remove desired Web services.
- Different services may be administered by different individuals. By isolating services (resulting in each host and service having a single administrator), you will minimize the possibility of conflicts between the administrators.
- The host can be configured to better suit the requirements of the particular service being provided. Different services might require different hardware and software configurations, which could lead to needless vulnerabilities or service restrictions.
- By reducing services, the number of logs and log entries is reduced so detecting anomalous behavior becomes easier.

How to do it

The suggested configuration principle is "deny first, then allow." That is, turn off as many services and applications as possible and then, selectively, turn on those that are essential.

➤ *Determine the functions that you intend to support with your Web server (e. g., cgi scripts).*

The number of services that are required on the selected host depends on the functions that you intend to provide on that host. This functionality could be for the Web, other services hosted on this computer, and the arrangements made for development and maintenance of the operating system and applications. Determine the configuration of the host with respect to

- file systems (e. g., whether any file servers will be used by this host)
- system maintenance (e. g., with multiuser systems, whether all maintenance will be done only via the console or remotely)

- server maintenance (e. g., if all the maintenance will be done on another host and only the resulting files downloaded to this host, there is no need to provide any compilers or editors on this host)
- network configuration (DNS vs. NIS)

➤ *If there are alternative ways of providing the same function, select the more secure way.*

For example, on UNIX systems, remote system maintenance (i.e., not from the console) can be provided using *remote shell* (`rsh`) or *secure shell* (`ssh`) capabilities; of the two, `ssh` is more secure.

➤ *Once the minimal set of services and applications has been determined, ensure that only those in the set are available on the host.*

Either do not install unnecessary services or turn them off and remove the corresponding files from the host. Be particularly careful with server programs—many of them can provide multiple services and will have to be configured to disable unneeded services. See the practice "Configure the Web server to enhance security" on page 15 for additional information.

➤ *After all configuration choices have been made, create and record cryptographic checksums or other integrity-checking baseline information for your critical system software.*

Policy considerations

Your organization's networked systems security policy should

- Require that public servers be configured to offer only essential services.

Other information

There can be different configurations of the server depending on the other features that the selected host operating system or environment provide. For example, certain operating systems provide extensive access control mechanisms that minimize or even avoid the possibility of unauthorized access at relatively fine levels of granularity.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p012.html`

5 *Configure the Web server to enhance security.*

When you install server software, you are normally presented with a number of choices for configuration options or preferences. Those choices should be made carefully to balance your security and operational requirements.

Also, the server host operating system may provide access controls for information stored on that host. This is particularly common on systems that support multiple simultaneous users. You should take advantage of these controls to help prevent the accessing and disclosure of information that is not intended to be published.

Why this is important

The requirements for public sites vary from one organization to another, so vendors of server software provide for configuring the software differently at each site. The default configuration settings may be optimized for a "typical" site, as imagined by the vendor, and may be based mostly on performance requirements or ease of installation. Usually, security requirements will necessitate a different configuration. Failure to change from the default configuration can reduce the security of your site.

A server host typically stores not only information intended for publication, but also a variety of other information that should not be published. This will normally include the server's log files as well as systems and applications software. On multiuser systems, it may include highly confidential information such as password files. If you are careful to use the access controls provided by the operating system on the server host machine, you can reduce the likelihood of inadvertent disclosure or corruption of that information.

How to do it

➤ *Configure the server's logging capability.*

The server log file records information about the server's behavior in response to each request. Analysis of the log can provide both business information (such as which Web pages are most popular) and security information.[1] There are many log file analysis tools available, most of which are designed to operate on a file in either of the two standard log formats (called "Common Log Format" and "Extended Common Log Format"). You should configure your server to create its log file in one of these formats.

The Common Log Format includes the name or IP address of the requesting

1. The practice "Inspect your system and network logs." on page 27 discusses using the log file to look for signs of attempted intrusions.

host, the user name supplied for access of password-protected pages, the data and time of the request, the http method of the request ("GET" or "POST"), the file requested, the http status returned by the server, and the number of bytes transferred. The Extended Common Log Format also includes the URL loaded by the requesting client immediately prior to the current request to your server, and the name of the client software of the requestor.

➤ *Configure auxiliary network services of the server.*

Some Web servers also provide other network services, such as serving files using the file transfer protocol (ftp) or gopher protocol, dispatching electronic mail, or accepting file uploads from Web clients. We recommend that all such services be disabled on the Web server, unless you have a compelling reason to use them.

➤ *Configure external programs executable by the server.*

Nearly all Web servers provide for the execution of external programs as a result of certain kinds of requests. These programs include common gateway interface (cgi) scripts, server plug-ins, security plug-ins, server applets, and perhaps others (depending on the particular server). The default configuration for your server is likely to have many such programs enabled.

Initially, you should disable all these auxiliary programs and then follow the procedures outlined in the practice "Offer only essential network services and operating system services on the server host machine." on page 13 to enable only essential programs.

➤ *Configure the server for local and/or remote administration.*

You should administer your Web site from the Web host console. Doing so eliminates the need for network traffic between the Web server (outside the firewall) and the administrator's workstation (inside the firewall).

However, there are many situations where this is not feasible, such as in organizations where the Web server is not easily accessible by the administrator. When you must do remote administration, choose a method that satisfies these requirements:

- The server host uses a strong method to authenticate the identity of the user who is initiating administrative processes. In particular, avoid authentication methods that require or allow the transmission of a password in clear text, unless it is a one-time password.
- The server host will allow remote administration from only one particular host.
- Network packets travelling between the administrator's host machine and the server would not, if intercepted, provide an intruder with information that would allow subsequent access to either the server or your organization's internal network.

➤ *Determine what access controls are provided by the operating system of your host machine.*

In particular, determine if you can limit file access of the Web services' processes. Those processes should be given read-only access to some files and no

access to other files. If these capabilities are not available on your host operating system, you can skip the next step.

➤ *Use the file access controls to achieve the following:*

- Public Web content files are readable but can't be written to by the processes that implement the Web service.
- The directories where that Web content is stored can't be written to by the server processes.
- Public Web content files can be written to only by the processes that allow for Web server administration.
- Web server log files can be written to by the server processes, but they cannot be read or served as Web content.
- Web server log files are readable only by administration processes.
- Any temporary files created by Web server processes (such as those that might be needed in the creation of dynamic Web pages) are limited to a particular subdirectory.

➤ *Disable the serving of file directory listings.*

The Web protocol (http) specifies that a URL ending in a slash character is treated as a request for a listing of the files in a directory. As a general rule, you should not allow your server to respond to such requests, even if all the files in the directory are intended to be public.

Such requests may indicate an attempt to locate information by means other than that designed for your Web site. Users may resort to this if they are having difficulty navigating through your site or if a link appears to be broken. Intruders may use this method in an attempt to locate information hidden by your Web site's interface. You may want to look for this kind of request in the server log files.

➤ *Configure the server so it cannot serve files that are outside the specified file directory tree.*

This may be a configuration choice in the server software itself, or it may be a choice in how the server process is seen by the operating system.

You should also take care to avoid the use of links or aliases in your file directory tree that point to files elsewhere on your server host or your network file system.

➤ *Make sure that the server cannot serve any of its own log files or configuration files as if they were public Web content files.*

Log files should be stored on the server host, rather than be sent to another host on your internal network. (However, you may want to keep offline archived copies of Web log files.)

Similarly, server configuration or preference files should also be kept on the server host.

In all cases, using both server configuration options and operating system access controls as appropriate, make sure that these files cannot be sent to

users, even if those users know the names (URLs) of those files. If possible, place these files outside the public data directory tree.

➤ *After all configuration choices have been made, create and record cryptographic checksums or other integrity-checking baseline information for your server software.*

Policy considerations

Your organization's networked systems security policy should

- Require that public servers be configured to enhance security.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p017.html`

6 *Consider the security implications when choosing external programs that the server can execute.*

In its most basic form, a Web server listens for a request and transmits the contents of the requested file over the network. However, several mechanisms have been created that increase the functionality of a Web server by allowing it to invoke other programs to operate on user-supplied data, resulting in delivery of specialized information to the user. Examples of these mechanisms are the common gateway interface (cgi) and server plug-ins. A Web server may also be able to execute a server applet, invoke a security plug-in, or upload files from the user's host.

You should consider security issues when making the decision to use such external programs.

Why this is important

All these forms of external programs can be added to the server at any time without having to modify the server code itself. External programs are widely available from many different sources, and they can offer valuable functionality for your public Web service. However, as a Web server administrator, you are likely to install a particular set of programs that results in a unique configuration—one that was not tested by the developers of the server software or the external programs.

Care must be taken in acquiring, installing, and operating these external programs. Otherwise, security vulnerabilities can be introduced, either as an inherent problem with a poorly written program or as an unexpected side effect of the installation of two or more programs. For example, many successful attacks on Web sites have exploited known vulnerabilities in commonly available cgi programs.

How to do it

➤ *When you need a particular functionality for your Web site, consider all the available ways of providing it. If you determine that an auxiliary executable program is appropriate, look for more than one source of programs that would supply the needed functionality.*

To the extent possible, assess the trustworthiness of the various sources of the programs you are considering. For example, you should have the least confidence in software from an unknown author and downloaded from an Internet source you do not know. If there are several programs that provide the needed functionality, choose one from a trustworthy source.

- *Verify that the copy of the program that you get (whatever the source) is an authentic copy.*

  Typically, you will need to use cryptographic checksums, digital signatures, or similar technologies.

- *Make sure that you understand all the functionality that a program provides. In particular, make sure that in addition to the capability you want, it does not include other capabilities you don't want.*

  Some kinds of programs, especially cgi scripts, are commonly distributed in source code form. If you have any doubts about the trustworthiness of the source or the authenticity of the code, submit the code to an appropriate technical review by knowledgeable people in your organization (or outside, if necessary).

- *Consult published information on security vulnerabilities to determine if any are known for your chosen program.*

- *Install the program on a test machine and test it to your own satisfaction.*

- *After installing the program, create new checksums or other integrity-checking baseline information for your server software.*

- *Pay particular attention to your server behavior and log files in the period immediately after you install the new program.*

Policy considerations

Your organization's networked systems security policy should:

- Require a security evaluation as part of your computing and network technology selection procedures.

Other information

CERT advisories and summaries[1] may from time to time include information on new vulnerabilities in Web server software.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p015.html`

1. See http://www.cert.org and ftp://info.cert.org/pub/cert_advisories/ .

7 Administer the Web server in a secure manner.

Administration of a Web server includes such tasks as transferring new content to the server, examining the server logs, installing new external programs, and otherwise changing the server configuration. These tasks usually can be performed either from the server console or from a separate host via a network connection. In either case, be sure to perform the tasks in a manner that does not offer opportunities for intruders to breach the security of the server.

Why this is important

Although the normal operational state of your server may be secure, during the performance of administrative tasks, your server may be in a vulnerable transient state. This is especially true if you choose to administer the server from a remote host, because this requires that you open a network connection through the firewall. Such a connection may be vulnerable to some forms of attack, and it may open the door to anyone on the Internet being able to "administer" your server. The result could be the loss of integrity of your Web content, an intruder gaining access to resources on your internal network, or an intruder being able to use your server as an intermediate host for attacks on other internal or external hosts.

How to do it

➤ *If you choose to administer the server from a remote host, you need to take precautions to do it in a secure manner.*

Choose a method that satisfies these requirements:

- The server host uses a strong method to authenticate the identity of the user who is initiating the administrative processes. In particular, avoid authentication methods that require the transmission of a password in clear text, unless it is a one-time password.
- The server host will allow administration from only one particular host. Authenticate the host in a manner that does not depend on network-resolved information such as IP addresses or DNS names, because intruders can falsify such information.
- Network packets travelling between the administrator's host machine and the server would not, if intercepted, provide an intruder with information that would allow subsequent access to either the server or your organization's internal network.

➤ *If it is feasible for your Web site, use a movable storage medium to transfer Web content from the authoritative copy to the public server.*

This could include a writable CD-ROM, diskette, hard disk cartridge, or tape. The advantage of this procedure is that it does not require a network connection through your firewall.

During the transfer, you may need to stop or disable your server. Some servers can be configured to continue operating, but to send a "Service temporarily unavailable" message in response to all requests.

Do not use a transfer method that mounts a file system from a host inside the firewall on the Web server host using NFS. There are inherent problems in the NFS protocol that could make that internal host vulnerable to attack.

➤ *If you choose to inspect the server log files from a host other than the server, use a secure method of transferring the logs to that host.*

Movable storage media and file encryption are two suitable methods.

➤ *After making any changes in server configuration or site content, create new cryptographic checksums or other integrity-checking baseline information for your server.*

Policy considerations

Your organization's networked systems security policy should:

- Require the use of secure procedures for administration of the public Web site.

Other information

There are two times when you need to update your Web server content:

- at a scheduled time, which may be monthly, weekly, daily, or hourly, depending on the nature of the material being published by your organization;
- immediately after you detect any breach of integrity of the content on the public server.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p016.html`

8 *Look for unexpected changes to directories and files.*

The file systems in your network environment contain a variety of software and data files. Unexpected changes in directories and files, especially those to which access is normally restricted, may be an indication that an intrusion has occurred. Changes may include modifying, creating, or deleting directories and files. What makes such changes *unexpected* may depend on who changed them and where, when, and how the changes were made.

Why this is important

Intruders often substitute, modify, and damage files on systems to which they have gained access. To hide their presence on your systems, it is common for intruders to replace system programs with substitutes that perform the same functions but exclude information that could reveal their illicit activities. They also often modify system log files to remove traces of their activities. By masking their presence on a compromised system, intruders prolong the time they have to use that system for their purposes. In several notable cases, the presence of intruders on compromised systems was not discovered until many months after the initial intrusion occurred.

Intruders may also create new files on your systems. For example, they may install *backdoor* programs or tools used to gain privileged access on the system. Intruders also make use of the disk space on compromised systems to store their tools and contraband.

Private data files and files containing mission-critical information are common targets of modification or corruption by intruders. Information about your organization that is accessible to the public or to subscribers via public networks and the Internet is also a common target. Several documented cases exist of prominent organizations that have had their Web sites modified to include offensive content and other erroneous information.

How to do it

➤ *Establish priorities and schedules.*

Examine the files on your system and prioritize the frequency with which they should be checked. The more mission- or security-critical the file, the more frequent the checking should be.

➤ *Maintain authoritative reference data for critical files and directories.*

For each file and directory, the authoritative reference data you maintain should provide enough information for you to be able to identify changes to

- location in the file system
- alternate paths to it, via links, aliases, or shortcuts
- contents of files, entries in directories
- exact size, and if possible, file system units allocated
- time and date indicating when the file or directory was created and last modified
- ownership and access permission settings, including execution privilege settings for software

Use robust cryptographic checksum technologies to generate a checksum for each file. Keep authoritative copies of files and checksums on write-protected or read-only media stored in a physically secure location.

➤ *Verify the integrity of directories and files according to your established schedule.*

Compare the attributes and contents of files and directories to the authoritative reference (either complete copies or cryptographic checksums). Identify any files and directories whose contents or other attributes have changed.

Always access authoritative reference information directly from its secured, read-only media. Never transmit authoritative reference information over unsecured network connections.

➤ *Identify any missing files or directories.*

➤ *Identify any new files and directories.*

Pay special attention to any new program files and their associated execution privilege settings.

➤ *Investigate any unexpected changes among those you have identified.*

If any changes cannot be attributed to authorized activity, initiate your intrusion-response procedures immediately.

Report the incident to your organization's designated security point of contact.

Policy considerations

Your organization's networked systems security policy should

- Define the responsibilities and authority of systems administrators and security personnel to examine file systems on a regular basis for unexpected changes. Users should be told about such authority and examination.
- Require users to report any unexpected changes to their software and data files to system administrators or your organization's designated security point of contact.

Other information

As authorized and expected changes are made to files and directories, you will need to perform your organization's procedures for securely updating your authoritative reference data.

Some kinds of important files are expected to change frequently (perhaps several times per second); these include system log files, transaction log files, and database tables. In general, the techniques described above will not be particularly useful in distinguishing normal changes to such files from those that might have been caused by intruders. Techniques based on transaction auditing are more useful in these cases.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p002.html`

9 *Inspect your system and network logs.*

Frequently, intruders leave traces of their actions in system log files. Hence, checking system and network log files periodically is one way to detect intrusions.

Why this is important

Logs may contain evidence of unusual and unexpected activities that have occurred on the system or network. Such log entries may indicate that someone has compromised or tried to compromise the system. By looking at log files on a regular basis, you may be able to identify attempted or successful intrusions soon after they occur and initiate the proper damage-prevention or containment procedures.

Background information

Log files vary depending on the operating system, application software running on the system, and logging configuration you have chosen. Multiuser operating systems often provide more extensive logging capabilities than do single-user operating systems. Table 1 describes information typically contained in logs.

Type of Log	Information Contained in the Log
user activity	• login activity • changes in user identity • file accesses by the user • authorization information • authentication information
process activity	• commands run by users • running-process information including program name, user, start and stop times, and execution parameters
system activity	• restarts and shutdowns of the system • administrative logins
network connections	• details (when, where, what kind) of connections attempted or established with the system • details of connections established from the system
network traffic monitoring	• records of all network traffic transactions

Type of Log	Information Contained in the Log
web server activity	• remote hostname or IP address • date and time of the request • request • response code indicating whether the request was successful or not • remote login name of the user (if available) • username which the user has authenticated himself under (if available)

How to do it

➤ *Periodically inspect each type of log file.*

We recommend that each log file be inspected at least daily.

Look for evidence of unusual or unexpected activity. One benefit of periodic inspections is that, over time, you will become increasingly familiar with the signs of *usual* and *expected* activity. This will make it easier to recognize the unusual and unexpected.

The table below summarizes unusual or unexpected activities that may be reported in each log type. For operating systems that support different levels of user privilege, be sure to look for unusual activity by users at all levels.

Type of Log	Unusual or Unexpected Activities
user activity	• repeated failed login attempts • logins from unexpected locations • logins at unusual times of day • unusual attempts to change user identity • unusual processes run by users • unauthorized attempts to access restricted files
process activity	• processes that are run at unexpected times • processes that have terminated prematurely • unusual processes (i.e., those not due to normal, authorized activities)
system activity	• unexpected shutdowns • unexpected reboots
network connections	• connections to or from unusual locations • repeated failed connection attempts and their origination and destination addresses and ports • connections made at unusual times • unexpected network traffic (i.e., contrary to your firewall configuration or unexpected traffic volume)

Type of Log	Unusual or Unexpected Activities
network traffic monitoring	• sweeps of your network address space for various services, indicating attempts to identify hosts on your network and the services they run • repeated half-open connections (may signify IP spoofing attempts, or denial of service activity) • successive attempts to connect to unusual services on your network's hosts • transactions originating outside your network with destinations also outside your network (signifying traffic that should not be traversing your network) • sequential (attempted) connections to specific services signifying someone trying to run network-probing tools against your networked systems
web server activity	• retrievals of information not expected to be available (e.g., directory listings, other files in the operating system) • repeated attempts to misuse the server (these may indicate someone trying to compromise your site) • flooding activities that could cause a denial of service problem (note the remote hostname or IP address)

➤ *Document any unusual entries that you discover.*

Over time, you may see recurring kinds of unusual log file entries. Maintaining records of such entries and what you determined to be their causes will help you and others to understand new occurrences more quickly and accurately.

➤ *Investigate each documented abnormality.*

Ask yourself questions such as

- Can it be explained by the activities of an authorized user? (e.g., the user really was in Cairo last week and connected to the network)
- Can it be explained by known system activity? (e.g., there was a power outage that caused the system to reboot)
- Can it be explained by authorized changes to programs? (e.g., the mail log showed abnormal behavior because the system programmer made a mistake when the software was modified)

➤ *Report all confirmed evidences of intrusion (or attempted intrusion) to your organization's internal security point of contact.*

➤ *Read security bulletins from trustworthy sources (e.g., CERT® advisories and summaries[1]) and other security publications regularly.*

This can increase your understanding of current intruder activities and methods, and you can use this information to improve what you look for in log files.

---

1. See http://www.cert.org and ftp://info.cert.org/pub/cert_advisories/ .

Policy considerations

Your organization's networked systems security policy should:

- Specify that log files be inspected on a regular basis by authorized personnel, and that anomalies be recorded and reported to your organization's designated security point of contact.

Other information

If your site has large networks of systems with many log files to inspect, consider using tools that collect and consolidate log file information. Over time, you will learn what is normal for your environment. You should integrate this knowledge into your site's specific procedures for inspecting log files.

Also, as you acquire, modify, or retire systems, your log review procedures may need to change. Make sure that your site's procedures are appropriate for your current technology.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

`http://www.cert.org/security-improvement/practices/p003.html`

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 1997	Final

4. TITLE AND SUBTITLE
Security for a Public Web Site

5. FUNDING NUMBERS
C — F19628-95-C-0003

6. AUTHOR(S)
Robert Firth, Gary Ford, Barbara Fraser, John Kochmar, Suresh Konda, John Richael, Derek Simmel, Lisa Cunningham

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-SIM-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.a DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12.b DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The module provides concrete, practical guidance to help organizations improve the security of their networked computer systems. It describes a set of practices that can increase the security of public web servers and the host organization's networks on which they reside.

14. SUBJECT TERMS
network security, Web server, World Wide Web

15. NUMBER OF PAGES
30 pp.

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL